Spokesman

AIR INTELLIGENCE AGENCY

Vol. 42, No. 3 March 2002

DEPARTMENTS

photo by Boyd Belcher

2nd Lt. (now 1st Lt.) April Ducote, crew commander at the Air Force Computer Emergency Response Team, a part of the 33rd Information Operations Squadron, works with members of the Air Force Information Warfare Center in support of a common mission. The agencies detect and identify network intrusive activity to prevent impact on Air Force network operations. See more photos and story on pages 8-12.

Brig. Gen. Paul Lebras
AIA commander

Maj. Steve Doub
Director, Public Affairs

TSgt. Marilyn C. Holliday
Editor

Special recognition goes to AIA unit public affairs representatives who submitted articles and salute inputs for this issue of Spokesman.

1st Lt. William Roschewski
MSgt. Walljasper
381st IS

SSgt. John Waldron
543rd IG

SSgt. Timothy Miller
303rd IS

MSgt. Alan Ambrose
26th IOG

2nd Lt. Mike Paluba
31st IS

Special thanks also to fellow public affairs offices:

Rob Young
NAIC

SMSgt. Fred Hagans
AFTAC

2nd Lt. Toni Tones
67th IOW

MSgt. Rick Corral
SSgt. Kristina Brown
70th IW

This funded Air Force newspaper is an authorized publication for the members of the U.S. military services. Contents of Spokesman are not necessarily the official views of, or endorsed by, the U.S. government, the Department of Defense, or the Department of the Air Force. The editorial content is edited, prepared and provided by the Public Affairs Office of the Air Intelligence Agency and its public affairs representatives throughout the command. All photographs are property of the U.S. Air Force, unless otherwise indicated. Send articles to AIA/PAI, Attn: Spokesman Editor, 102 Hall Blvd., Ste. 234, San Antonio, Texas 78243-7036.

Teamwork guarantees future successes

"We're flooding people with information. We need to feed it through a processor. A human must turn information into intelligence or knowledge. We've tended to forget that no computer will ever ask a new question."

Retired U.S. Navy Rear Admiral
Grace Hopper

By Brig. Gen. Paul Lebras
AIA commander
Lackland AFB, Texas

As I take command of the Air Intelligence Agency, I am struck by the relevance of Admiral Hopper's quote. Did you ever do a search on the web or INTELINK and end up with 3,000 hits? Not very helpful, was it? It sure wasn't to me.

We are on the cutting edge of the information age, but it is people who must make sense of the data. In the first place, we need smart people to manage existing information – developing knowledge bases rather than databases, working push-pull architectures – so that we make the output immediately relevant to the mission. We also need people who can make sense of the raw data, be it radar imagery, bits and bytes, or electromagnetic emissions, so that we provide understanding of what the data means. In both cases, AIA excels.

In my last tour at AIA, as the vice commander, I was tremendously impressed with the quality of our people: officer and enlisted, military and civilian, government and contractor.

One time I received a demonstration on a nodal analysis capability. The automated tools were very sophisticated, but it was the depth of expertise and understanding that impressed me the most. I remember thinking, "Other organizations which purport to do this mission are mere amateurs compared to this crew."

Time after time, the people of AIA – at the headquarters, at the centers, in our operational units – demonstrate that same degree of expertise. You would be hard-pressed to find an organization that epitomizes our core value of "Excellence in all we do," more than AIA. We'll need that excellence for the tough challenges ahead.

The first and most important of these is the global war on terrorism. There are many aspects of this fight that will take us into new territory, both literally and figuratively. For example, we may well be operating in regions of the world where we do not have much experience; what type of linguists will we need?

We face an amorphous enemy, which operates in the shadows. It is a far more difficult task to template a worldwide terrorist network like al Qaida than it is a conventional integrated air defense system. How do we do intelligence preparation of the battlespace in all its dimensions – physical, electronic, human factors, cyber – to gain predictive battlespace awareness of a non-traditional enemy that focuses on asymmetric warfare?

Luckily, many of the processes we've built over the years provide a guide. Just look at the parallels between computer network defense and the war on terrorism. Both are global phenomenon that cut across the traditional boundaries among our combatant commands.

Both generate a tremendous amount of "noise," which serves to mask real threats among thousands of false reports. Both require detailed skills – technical in one case, cultural and geographic in the other. Given these parallels, there may be lessons we can transfer from one mission area to the other. At the same time, many of our more traditional missions will continue to be critical to winning the fight. Consider the role that signals intelligence and imagery analysis played in the successful prosecution of Operation Enduring Freedom.

The second major challenge we face is completing the integration of AIA into 8th Air Force and Air Combat Command. Some elements of AIA have been part of the ACC team for many years. Our intelligence squadrons flying the RC-135/ Rivet Joint and working the U-2 mission have long been under the operational control of ACC to ensure that we deal with

Brig. Gen. Paul Lebras

platforms and their end-to-end connectivity as a weapons system.

Even when our units did not have a formal command relationship with ACC, we played a key role in meeting ACC's mission needs. When I was the ACC/IN, I remember the great work that the 480th Intelligence Group did for the command. It included everything from helping to spin up air expeditionary forces for deployment to ensuring the F-117 got the imagery it needed. The major change is that we have now made these relationships formal, and our centers are now part of the larger ACC team.

AFDD 2-5 describes the unbreakable link between intelligence, surveillance and reconnaissance and information warfare in executing information operations. The ACC/8AF/AIA team is the nexus of this doctrine as information warfare flights, supported by the Information Operations Center serve A2, A3 and A6 decision makers.

The key to achieving success in both the above challenges is teamwork across the board: within AIA, between AIA and the rest of ACC and with the national intelligence community.

Just like the Cold War, successful prosecution of the war on terrorism will require a string of interconnected processes. For kinetic kills, this might include measurement and signature analysis to determine activity levels, pre-strike imag

commander's comment's

ery, precise geodetic coordinates, technical data on enemy air defense systems, SIGINT situational awareness for jets in the fight, and more.

Every single link in this chain is critical; if one piece is incomplete or incorrect, the mission fails. If the geodetic coordinates are wrong, a precision-guided weapon will miss the target; if the air defense analysis is wrong, the strike aircraft may never get to the target – you get the idea.

The criticality of the processes means that every person in the chain is critical – no single function is any more or less important that the others – and that demands teamwork.

The AIA-ACC integration demands similar teamwork. As a first lieutenant, I learned firsthand the value of staff work and coordination from a World War II fighter who was my boss. I've carried his lessons with me for over 25 years: it's far easier to resolve issues before a message is sent than to do damage control after it's transmitted. I learned to ask myself questions such as "What other organizations have equity in the project or process I'm working?" and "How should I route this message or staff action?"

By asking such questions, we can ensure that the integration proceeds in a spirit of coordination and cooperation to achieve the common mission.

On Sept. 20, 2001, President Bush stated "Whether we bring our enemies to justice or bring justice to our enemies, justice will be done."

Our AIA team is contributing every day to this fight, and I look forward to leading all of you as we continue to carry out the president's words.

names in the news

Hospice volunteers spread a little cheer

By SSgt. John Waldron
543rd IG
Lackland AFB, Texas

Alfredo De La Cruz recently spent an afternoon joking and playing checkers with TSgt. Crist Middaugh, a volunteer from the Santa Rosa Hospice Program

Four days later the retired painter passed away after a hard-fought battle against pulmonary fibrosis.

Middaugh, who is stationed with the 543rd Intelligence Group at Lackland AFB, Texas, said working as a hospice volunteer gives him an opportunity to show love to patients like De La Cruz who are suffering from terminal illnesses.

"It is amazing to me how much of an impact you can make by visiting someone a few hours every week," Middaugh said. He started volunteering after his wife, Denise, accepted a full-time position with the program last fall.

He said patients and their families participating in hospice programs look forward to the visits.

"A few months ago we had a birthday party for one of our patients who was turning 94," he explained. "After the party, her son pulled me aside and told me that it was the first time in a month that she was alert and responding to the people around her."

The Santa Rosa program is one of 13 hospice programs in the San Antonio area that reach out to local residents, according to Denise Middaugh, volunteer coordinator for the Santa Rosa program.

She said the types of patients involved in hospice vary dramatically.

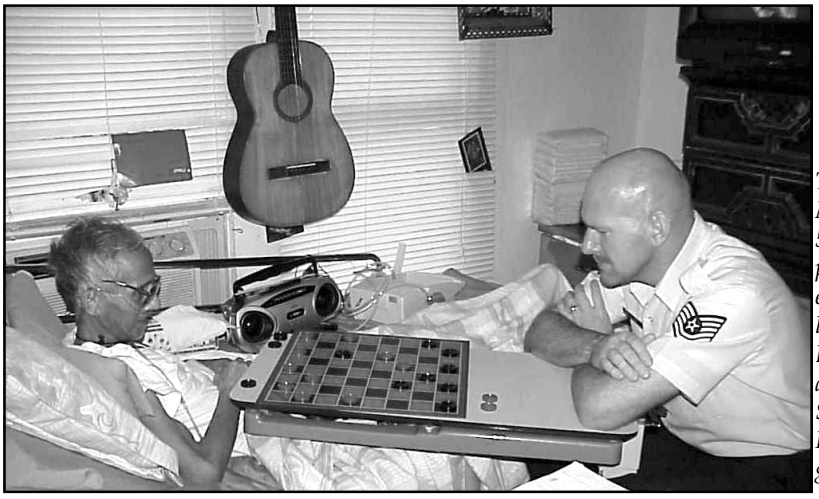
"Our oldest patient is 94 years old and our youngest patient is a 7-month-old infant," she explained.

According to Middaugh, the 40 hospice volunteers currently serving in the program work in a variety of areas.

"Hospice can mean everything from providing patients with companionship to delivering food during the holidays to families caring for a sick relative," she commented.

The demand for hospice volunteers, according to Middaugh, continues to grow.

"People have no idea what a difference an hour of their time can make to someone," she said. "Just sitting with a visitor and talking can bring a hospice patient so much joy."



TSgt Crist Middaugh, 543 IG, plays checkers with the late Alfredo De La Cruz as part of the Santa Rosa Hospice Program.

Brooks commander honors 68th IOS for contributions after Sept. 11

By Rudy Purificato
311th Human Systems Wing
Brooks AFB, Texas

Two Brooks AFB units earned their first 311th Human Systems Wing Commander's Awards recently for their post-Sept.11 contributions made in support of America's new war on terrorism.

For only the third time in the award's history, the base's highest honor was presented to two separate winners simultaneously.

The 68th Information Operations Squadron's Operations Flight and the 311th Security Forces Squadron shared the spotlight as the November and December award recipients, respectively, during a twin ceremony presided by Brig. Gen. Lloyd Dodd, 311th HSW commander, Jan. 11.

The 68th IOS was recognized for operations security support that its 68-member operations flight provided to unified and major commands during Operations Enduring Freedom and Noble Eagle.

Operations Flight personnel, who were deployed to eight locations, monitored 67,483 telephone calls and 235,918 e-mails that resulted in the interception of 759 reportable security disclosures.

As a consequence of their identifying force protection and defensive information vulnerabilities, several OPSEC security changes have been implemented, noted Maj. Carlos Bushman, 68th IOS director of operations.

Lt. Col. Steven "Remo" Payson, 68th IOS commander, said, "They (Operations Flight) are definitely making an impact on the security postures of DoD warfighters embroiled in ongoing operations. This flight's successes are the epitome of this unit's motto, 'Determination in Spirit'."

Col. Terry Nelsen, 311th Air Base Group commander, was equally effusive in praise for the 311th Security Forces Squadron. "During October 2001, the 311th SFS provided exceptional mission support for Brooks AFB in the wake of the terrorist attacks in the United States. The squadron maintained rock-solid security while in force protection conditions throughout the entire month," Nelson noted.

Det 2 celebrates Vets Day in Germany

Detachment 2, 26th Information Operations Group, Bad Aibling Station, Germany, commemorated Veteran's Day with German and British troops Nov. 11.

Ceremonies were held at a German cemetery near the village of Gmund and at the British cemetery near Durnbach.

Bad Aibling Station was represented by a multi-service formation during ceremonies held at both locations. The station's participation in this year's ceremonies was organized and coordinated by MSgt. Scott Van Voorst, detachment superintendent.

It was a clear but very cold morning as the members of the formation braved the elements to pay their respects to the fallen comrades of previous wars.

Detachment members participating were: MSgt. Scott Van Voorst, TSgt. Tracy Currier, SSgt. Leonard Battle, SSgt. Brian Stolpe and A1C Ryan Rode.

TSgt. Mitchell Ross, 694th IG/DO, prepares to be STEP promoted by Lt. Gen. Thomas J. Keck, 8th Air Force commander, and Col. Harold J. Beatty, 70th Intelligence Wing commander, during a surprise ceremony at Fort Meade, Md. Keck presented the Stripes for Exceptional Performers stripe as Ross was briefing him as part of a familiarization slide show presentation.

"It took me totally by surprise," Ross said. "I was giving the briefing and then the general started asking questions with a firm attitude. I was prepared for the questions, but the promotion was quite a shock.

"It was hard grilling this young man with a straight face," Keck said. "I had four stripes to give out command-wide and Sergeant Ross was certainly deserving of one."

Skivvy Niners, Koreans celebrate 20 years of cooperation

By 2nd Lt. Stephanie Oldham
303rd IS
Osan AB, ROK

September 2001 marked the 20th anniversary of the cooperative agreement between the Republic of Korea's 1925th Armed Forces Unit and the U.S .Air Force's 303rd Intelligence Squadron, more commonly known as Skivvy Nine. During their years of working together at Osan Air Base the two units have developed a complementary relationship, producing a blend of intelligence capabilities found nowhere else in the world.

At a commemorative ceremony Sept. 5, the unit commanders spoke of 20 years of accomplishments. Lt. Col. Kevin Hopkins, 303rd IS commander, referenced the recently-concluded Ulchi Focus Lens exercise, saying "we demonstrated that U.S. and South Korean forces can quickly form an effective military team that can meet the goals of our two countries." Hopkins went on to highlight that the 1925th AFU exemplify that teamwork every day of the year.

"Today, Skivvy Nine sits side-by-side in the workplace with the 1925th AFU. The 1925th's team brings indispensable assets to the mission. They provide portions of the intelligence picture that enable Skivvy Nine to inform and protect the warfighter and execute operations on a daily basis. The South Koreans' experience and knowledge provide continuity that is critical in an environment with such rapid turnover of U.S. personnel. Highly professional and dedicated to the defense of their homeland, 1925th troops take a personal interest in the success of the unit," he said.

At the ceremony, 1925th AFU Commander Lt. Col. Hwang Ki Young recognized outstanding performers. Skivvy Nine's awardees included Capt. Winston Lee, flight commander of C4 Systems. He received a letter of appreciation from the Ministry of National Defense.

The 1925th commander also recognized MSgt. Michael Donovan, chief of Mission Management, MSgt. Christopher Hoak, Baker Flight superintendent, and MSgt. Robert Wilhoyt, Charlie Flight ground mission supervisor.

A luncheon following the ceremony offered a colorful abundance of traditional Korean dishes. The commanders toasted the shared past and collective future. Later in the afternoon, Korean troops and American guests competed in a game of soccer.

Fifty years ago American and Korean men died side by side on the hills that are home to Osan. Twenty years ago then-commander of Electronic Security Command Maj. Gen. Doyle Larson helped celebrate the founding of the 1925th AFU, and today the relationship between the 1925th AFU and the 303rd IS exemplifies a continued spirit of cooperation. As Hwang said, "although we are from different environments in customs and languages, we have kept a remarkable relationship as true partners. Now it is time to raise the spirit of combined operations to a higher level, and achieve splendid results in operations through understanding and cooperating with one another."

"The demands of the mission at Osan require commitment to a fast-paced and hard-working lifestyle," Hopkins said. "Unfortunately, one common casualty of this dedication is appreciation for the rich history of the streets we walk on. Many people pass by Hill 180 every day, often forgetting that they are passing by a legendary battlefield, and the home of a legendary unit."

"Since its establishment at Taegu in 1950, Skivvy Nine has made a name for itself worldwide," Hopkins said. "The squadron is no less famous for its exceptional operational performance than for its prevailing sense of camaraderie. Skivvy-niners gather for reunions decades after leaving the Korean peninsula."

End of an era: CIOs retired

Technology takes place of humans

By SrA. Connie Bias
3rd Wing Public Affairs
Elmendorf AFB, Alaska

Technology has, once again, taken over.

This time, it has replaced humans entirely, taking the human element out of the combat information operators program. While the technological advances will improve mission accomplishment and effectiveness, they are also bringing about the end of an era of service stretching from the darkest days of the Cold War to present-day operations like Northern and Southern Watch in Southwest Asia and, more recently, Noble Eagle.

Since the early 1980s, CIOs, also known as area specialists, have flown aboard the E-3 Sentry AWACS on missions spanning the globe. The operators' primary tasks involved applying their extensive knowledge of theater forces to reconnaissance, providing their unique expertise to the aircrews to which they were temporarily assigned.

"The CIO program was permanently established here in 1987 with the activation of the 962nd Airborne Air Control Squadron," said former operator TSgt. Ken Shannon from the 381st Intelligence Squadron. "We maintained a year-round presence in Operation Southern Watch, as well as the Alaskan theater, including Operations Northern Denial and Noble Eagle."

While the abiding security restrictions preclude the former operators from going into much detail about their responsibilities and experiences, they're proud to have made an impact, according to Shannon, whose career was enriched by his accomplishments and experience.

"I think the position was quite useful, and I had the opportunity to revisit Southwest Asia, and see firsthand what remained to be done after Operation Desert Storm," he said.

Throughout the years, CIOs have participated in more than 100 exercises, including Fencing Brave, Cope Thunder and Northern Edge. The Area Specialists have also supported multiple operations including Desert Shield and Desert Fox. More than 25 Area Specialists at Elmendorf have flown more than 650 mission and 4,500 hours since the program began here.

One of those specialists, TSgt. Ernest Parrish, leaves a legacy of faithful military service. Parrish died in the Sept. 25, 1995, Yukla-27 crash at Elmendorf. Parrish Hall on Security Hill in San Antonio, Texas, honors his service.

Now the CIO program is also a legacy. In September, Headquarters Air Combat Command announced the termination of area specialist support to AWACS, and the program ended in December.

A group of Elmendorf area specialists completed a different sort of "fini flight" a couple days after Christmas, flying their final mission Dec. 27.

"Technological advances to the E-3 Sentry's mission systems drove closure of the program," said Shannon. But that doesn't mean the end of a career for him or the other CIOs, or that he's pessimistic about the future. In fact, Shannon said the program's closure has "zero effect" on his career and military future. Shannon is looking forward to more of what he gained from his time as a CIO - the opportunity to make an impact while continuing to experience the rich life the Air Force has to offer.

Shannon now has the opportunity to return to the Defense Threat Reduction Agency to participate in missions in support of the Open Skies treaty, which became enforceable Jan. 1.

"The single thing I will miss most (about being a CIO) is being assigned to Alaska. However, Elmendorf is designated to host Open Skies observation flights and aircrews, so you haven't seen the end of me just yet," he said.

Nor have we seen the last of the proud men and women who served as CIOs. Like Shannon, they'll be lending their expertise and professionalism to other vital disciplines.

AFIWC, AFCERT team up for common mission

By Capt. Tre Martin
AFIWC/IOT
Lackland AFB, Texas

It's 8 a.m

Chet Wall walks through an endless maze of cables and computers, painstakingly evaluating the latest and greatest technologies. Virtual private networks, network traffic analyzers, and intrusion detection sensors.

The very success of his organization hinges on his ability to plan and arrange these technologies to serve and protect its information.

His modus operandi must always be the same: Always stay one step ahead of the competition.

No, Chet is not some company's highly-paid CIO.

It's 3 p.m.

Chad Cooper gathers information on activities and places that the average person never hears about.

He carefully draws parallels between certain events and actions, linking them to corresponding people and organizations.

His bosses require him to master keen problem-solving skills to gather the information their organization requires.

No, Chad is not a top-secret spy.

It's 2 a.m.

April Ducote sits in front of her computer utilizing various administrative network tools to analyze hundreds of IP addresses. She visits an assortment of hacker websites gathering information on a myriad of system backdoors and vulnerabilities.

April realizes that success lies in the minute details, therefore she knows that all it takes is one carefully planned connection or one careless action by a system administrator and root access will be achieved. She patiently awaits the inevitable.

No, April is not some foreign-based hacker.

The fact is that Chet Wall and Chad Cooper are first lieutenants stationed at Lackland AFB, Texas, in the Air Force Information Warfare

photo by Boyd Belcher
1st Lt. Chet Wall is a countermeasures officer and technical project lead in the Information Operations Technology Division . From left are, Wall, Carlos Garcia, Alva Veach, Juan Munoz, Harry Halladay, Robert Coursey, Dustin Childs, Chris Hernandez, Philip Soliz and Wayne Rodriguez.

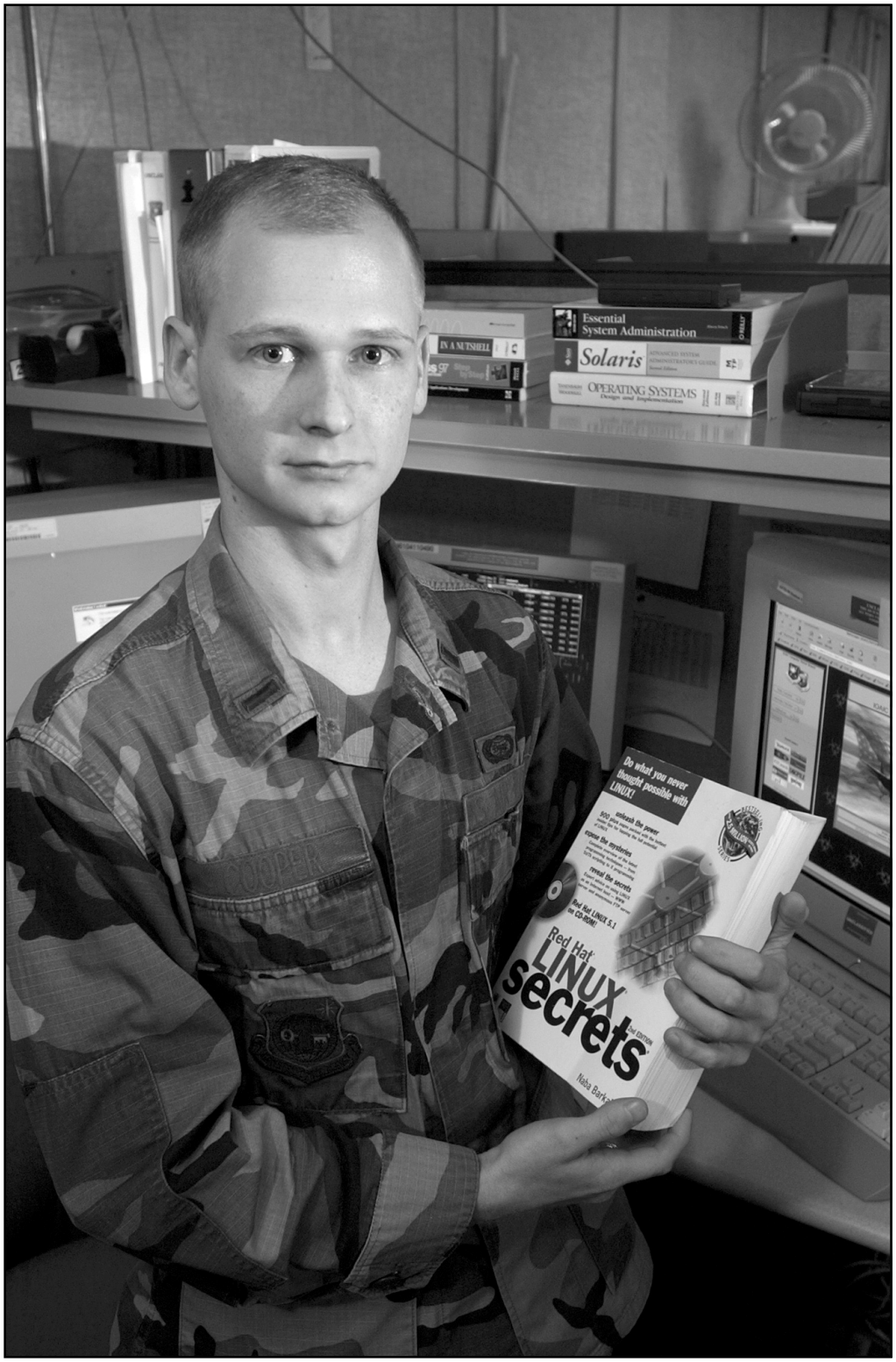


photo by Boyd Belcher

1st Lt. Chad Cooper is the officer in charge of the Computer Threat Section in the Information Operations Analysis Division of the Air Force Information Warfare Center.

Center. Wall is a countermeasures officer and technical project lead in the Information Operations Technology Division . Cooper is the officer in charge of the Computer Threat Section in the Information Operations Analysis Division. They support AFIWC's mission to develop weapon systems and threat analysis products to support computer network defense operators such as 1st Lt. April Ducote, a crew commander at the Air Force Computer Emergency Response Team, a part of the 33rd Information Operations Squadron.

Their efforts illustrate a finely tuned synergy between AFIWC and AFCERT in support of a common mission: detect and identify network intrusive activity to prevent impact on Air Force network operations — a mission far easier said than done.

Members of AFIWC accomplish this mission every single day, ensuring the Air Force leads the charge in America's relentless cyber war. Air Force information and information systems are vulnerable to attack and require aggressive defensive counter-information programs and capabilities to deter and respond appropriately to both foreign and domestic threats.

In many cases, information that the AFIWC deals with on a daily basis can simultaneously be a weapon and a target. AFIWC carries out its mission with this firmly embedded mindset. Where as IOT creates technology solutions to address threats and vulnerabilities, IOA's main focus is using these solutions and other methods in identifying these threats and preventing them from succeeding.

IOT provides a wide range of defensive information warfare technology solutions and develops the foremost safeguards for the Air Force worldwide network.

As one of the nation's early pioneers in information assurance, AFIWC began development of an intrusion detection system in 1991 and three years later, released its IDS prototype. "Many people don't understand that before AFIWC's

photo by Boyd Belcher
Christine Heikkinen is a computer threat intelligence analyst with the AFIWC/IOA.

collaboration with University of California, Davis and Lawrence Livermore National Labs, there was no intrusion detection on the network level," Capt. Sam Birch, chief countermeasure architect in IOT, said. "There was practically no commercial industry before us."

Beneficial collaboration has only grown over the years. AFIWC works together and shares technical information with a variety of organizations including Joint Task Force-Computer Network Operations, the National Information Protection Center and various law enforcement agencies, research institutions and academia.

IOT has mastered the difficult art of staying on technology's cutting edge. Other successes include the deployment of a virtual private network to more than 150 locations; research into desktop firewalls, and efforts to defend telecommunications from attack.

Yet, it is the Automated Security Incident Measurement Sensor, Common Intrusion Detection Director System, and the Computer Security Assistance Program Database System that have thrust the Air Force to the very forefront of the intrusion detection community. These three pieces form the heart and soul of the Department of Defense's premier IDS.

"It is one of our highest priorities in the AFIWC to develop and deliver the absolute best IDS that we can," Col. John Wright, AFIWC Information Operations director, said. "The criticality of a robust intrusion detection system must not be understated for our Air Force warfighters' information needs."

One might ask what exactly is an IDS and how does it work? Whereas a firewall acts much like a lock on a door, IDS tools act as the security guard in charge of watching that lock. They constantly scan network traffic or host audit logs and look for anything unusual, normally defined as something outside the parameters of an organizations security policy.

The AFIWC-developed ASIM sensor, CIDDS, and CDS decision support system make up the operational network-based IDS in use today. The ASIM sensor performs much like a network sniffer. Installed on the digital perimeter of a base's network, the sensor analyzes packets of information flowing into and out of the base and forwards unusual activity such as unwarranted port scans or random connections from unidentified sources. There are more than 150 sensors in operation across the Air

Force. Real-time alerts are forwarded from the sensor directly to a CIDDS, more commonly known as a director. Each major command has an operational director, which in turn reports its real-time data to the main parent director located at the AFCERT.

The director correlates the ASIMs information into a database and graphically portrays and manipulates this data through a user-friendly interface.

"For analysis purposes, nothing matches the capabilities of the director," Capt. Chuck Port, the AFCERT's Incident Response Team chief, said. "Commercial products can give us alerts, but not the data to back up what is happening. I think commercial sectors are catching up but the Air Force is clearly at the forefront."

The third piece to this IDS puzzle is the decision-support system known as CDS. This centralized, web-based repository allows the Air Force cyber warrior to access virtually any element of information ranging from past hacker incidents to virus information to Air Force-regulated procedures and policies.

It also provides the analyst with fingertip access to Air Force and MAJCOM numerical statistics for hacker incidents and virus attacks as well as a whole plethora of other database queries. AFIWC's combination of the sensor, the director, and decision-support system has provided the most bang for the buck for CND units.

While IOT formulates the technical solutions that provide evidence of malicious activity against the networks, IOA teams with AFCERT to play the role of the clever detective, masterfully identifying what person or organization is behind a particular activity.

"We identify who the hackers are on a tactical basis," David Lemmon, chief of the IOA Computer Network Operations Threat Analysis Section, said. "Identifying the who behind these electronic attacks is like being a Sherlock Holmes — every event is like a little mystery to solve."

IOA's primary focus is investigating foreign threats on a non-structured, semi-structured, and fully-structured basis, which covers activity initiated by beginning "script kiddies" all the way up to government-sponsored activity.

Investigating foreign threats is accomplished in two distinct phases. First, the computer threat team works with the Joint Threat Incident Database, which obtains and correlates as much information as possible on all unidentified foreign network actions. Their analysis becomes the basis for recommendations for AFCERT action and is simultaneously sent to higher joint levels, such as the Joint Task Force-Computer Network Operations.

The second phase involves the Computer Threat Analysis Tool, which focuses on creating target profiles of active foreign hacker groups, internet service providers and associated organizations.

These profiles are usually one- to two-page summaries of a particular group or organization posing a threat to Air Force or DoD information systems. The AFIWC/IOA CTAT crew correlates the most serious foreign technical activity and its corresponding relationship to real-world events.

AFIWC analysts share the data and their analysis with other organizations including national agencies, the Joint Information Operations Center and the Air Force Office of Special Investigations.

The JTID tool is so effective that the United States Space Command adopted it as its standard for computer network intelligence production. Essentially, the gathering and sharing of this target profile information across the DoD network security community is IOA's main goal—one they accomplish on a daily basis.

The collaborative efforts of the AFIWC teams have produced an unparalleled intrusion detection system and analysis process. However, technology can only accomplish so much.

Whereas AFIWC's ASIM/CIDDS/CDS tool suite can provide the data, no physical IDS system can analyze the massive amount of incessant, incoming information to ultimately provide that magic silver bullet that addresses all security worries.

The fourth, and most important "X factor" in the whole IDS equation is the human mind.

In the commercial sector, one of the most critically unsung problems in terms of computer security is the lack

The nation's cyberwar may not produce the visual bomb blasts that we see on CNN or FOX News, but this war is as intense as any other kinetic activity.

of talented individuals to protect information systems from attack.

Fortunately, the AFIWC possesses some of the most highly skilled security and technically adept minds in the country. And in the ultra fast-paced computer security realm, having well-trained analysts who have the ability to learn and process information quickly is an absolute must.

Because IOA's JTID has become the standard for all joint-level databases of its kind, personnel come from every level and service to learn from the AFIWC's members, Lemmon said.

IOA analysts do not just rely on the IDS tools and their training to accomplish the mission—they often turn to each other.

At any given time, foreign threats could launch a merciless attack against the Air Force's electronic forces, such as from China shortly after the P-3 incident last year. Having a diverse staff of analysts provides a seasoned line of defense in such situations.

The IDS tool suite, used by trained analysts, has produced innumerable results that have greatly benefited the Air Force.

AFIWC/IOA, teaming with AFCERT, became the first ones to identify the Lion Worm, a foreign created virus that once enabled on a system would send critical network information to a domain in China. Their teamwork resulted in the eventual capture of the virus creator.

The nation's cyberwar may not produce the visual bomb blasts that we see on CNN or FOX News, but this war is as intense as any other kinetic activity.

Fortunately, with people like Wall Cooper and Ducote leading the planning and analysis of our cyber fight, we can all take heart that the United States Air Force's CND units will always stay one step ahead of the game.

Mission system without security paints scary picture

By Paul Woeppel,1st Lt. Christopher Betz & 2nd Lt. Kim Evans
690th ISS
Lackland AFB, Texas

Often, information assurance is viewed as a hurdle to overcome, not an integral part of the system or mission.

But listen to the news and you hear of another person being arrested for spying and stealing government information. The "insider threat" of spies is real with the arrest of Robert Hanssen from the FBI and Ana Belen Montes, who worked for the Defense Intelligence Agency.

These individuals were properly cleared and had access to secure working areas or Sensitive Compartmented Information Facilities and classified information. It makes you wonder "how secure are our information systems?" when it comes to protecting our data.

As the military enters into a new mission to eradicate the threat of terrorism in the world, the reliance on Sensitive Compartmented Information information systems have become the focal point of intelligence gathering. So who is tasked to ensure that these classified systems are set-up, maintained, and operated securely?

Actually, two organizations are responsible for managing this program. The 690th Intelligence Support Squadron's Information Protection Flight manages the accreditation of all information systems for the Air Intelligence Agency on behalf of the National Security Agency.

The second organization is the Air Force Service Certifying Organization, which is aligned under AC2ISRC/A-26. They are tasked with certifying and accrediting SCI systems for Air Force and Air Force-supported joint commands on behalf of the DIA. This includes all Air Force-unique SCI systems and numerous migration systems for which the Air Force is executive agent.

The 690th ISS/PIA and AFSCO are required to ensure that all SCI information systems comply with Director of Central Intelligence Directive 6/3. This document outlines the requirements necessary to ensure the confidentiality, integrity, and availability of these systems to process SCI information without compromise to their security.

Additionally, they ensure that the systems are configured with the best possible security safeguards and mechanisms. This includes incorporating new technology vulnerability and assessment tools into their computer security test and evaluations.

Government members and contractors who develop classified systems must understand security requirements and implement them correctly before getting the final stamp of approval.

The idea of a mission system without security can create a scary picture. Just imagine someone gaining access to your information, and you never knew it. One way to ensure

major security incidents don't occur is to get the appropriate certification and accreditation office involved.

Currently, both 690th ISS/PIA and AFSCO are located at Lackland AFB. They work hand in hand ensuring there is one focal point for all certification and accreditation issues for SCI systems.

The question is always asked, "Why do we need to do certification and accrediation?" A good analogy is driving a vehicle. In order to drive we must first get a valid state driver's license. The license certifies that the person is qualified by the state to operate a vehicle. Obtaining a driver's license is equivalent to the certification process.

Similarly, the information system certification process ensures that the system meets the security architecture of the network on which it will reside.

In obtaining a driver's license a person needs to understand the driving laws to pass the test. This is also the case during the certification process.

The people involved need to understand the rules and requirements for developing an information system, apply them, and then test the system to ensure it meets the requirements. This is accomplished by verifying that all the latest security patches and service packs are applied, turning off any network services that are not needed, and closing any ports that do not need to be used.

Additionally, we are required to have license plates and a state inspection on the vehicle we plan to drive.

The same can be said for the accreditation process. It provides the same authorization for systems operating on networks. During the accreditation process, a review of the system is conducted to ensure that the appropriate documentation, security testing, and network authorization have been granted to allow the system to operate.

The overall goal of the C&A process is to ensure that the system that is developed and ultimately connected to the network be as secure as possible.

If this process did not occur, hackers and spies would be able to find back doors into systems and steal personal or critical mission information that might have life threatening impacts. Also, networks may come to a halt or slow down if the system utilized more bandwidth than the network can support. These are only a few of the potential problems if the system is not certified and accredited. The C&A process protects the networks from these problems and ensures safe operation on the network.

The individuals tasked with becoming the information systems security manager and the information system security officer are responsible to the senior intelligence officer or the commander for verifying that security of their information systems is properly configured, and the appropriate certification and accreditation paperwork is maintained.

This responsibility is usually done as an extra duty; therefore, it is imperative that the senior intelligence officer and commander provide their support and emphasize the importance of this mission.

The certification and accreditation of SCI systems is not intended to interfere with or hamper the operational mission. The process is designed to ensure that there is no compromise of classified information that could lead to harmful repercussions against US personnel.

Given the current operational tempo, the information assurance community and the operational community can develop a smart method for accomplishing the much-needed certifications and accreditations.

An informative Systems Security Checklist is available from the following address:

690th Intelligence Support Squadron Information Protection Flight & Air Force Service Certifying Organization
102 Hall Blvd Suite 104Q
Lackland AFB, TX 78243

For more information, call DSN 969-3396 or (210) 977-3396. The website address is http://aiaweb.aia.af.mil/homepages/690iss/pi/pihome.html.

The overall goal of the certification & accreditation process is to ensure that the system that is developed and ultimately connected to the network be as secure as possible.

ACC command chief makes time to visit Pacific-based units

By SMSgt. Tim O'Grady
692nd IOG
Hickam AFB, Hawaii

What does it take for the Air Combat Command senior enlisted leader to visit his Pacific Air Force-based troops? About 14 days, nearly 18,300 miles in the air, close to 10 hours driving the Korean countryside, and a whole lot of jet lag.

That's exactly what CMSgt. Dan Keane, ACC's command chief master sergeant experienced during his recent visit to several ACC units that call the Pacific theater home.

During what's been dubbed "PACAF Tour 2002," the chief spent time at Yongsan Army Garrison, Osan Air Base, and Wonju Air Station, Republic of Korea; Kadena Air Base, Okinawa Japan; and Hawaii-based units either stationed at or supported by Hickam AFB.

For Keane, the trip was a series of firsts that started shortly after he left his home base at Langley AFB, Va.

"I'd never been farther west than California before. I'd never been around some of the AFSCs I ran across on the trip, and I never tried eating with chopsticks before," said Keane.

After a long flight that involved crossing the international dateline and several airplane changes, Keane hit the ground running at Yongsan Army Garrison, where he visited with troops assigned to the Special U.S. Liaison Activity Korea.

After a brief visit to the work centers, where U.S. forces work along side their Korean counterparts, the chief was off to Osan Air Base, home to "Skivvy 9," and the 7th Information Warfare Flight. While at Osan, Keane also took time to visit with members of the 5th Reconnaissance Squadron.

Keane donned headsets and attempted to copy code and translate foreign languages during a simulated mission. It didn't take long for the chief to understand why the training regimen for many of the airborne operators was so intense.

Next stop, Wonju Air Station, Republic of Korea. With just a dozen buildings and less than three acres of real estate, Wonju could very well be the smallest Air Force installation in the world. It certainly was another first for the chief, who got a quick lesson in seismology and quickly learned that field work in Korea involves more than just driving on paved roads.

"I must admit, I was almost concerned when we started crossing partly frozen streams, climbing up the sides of steep hills and crossing fields with no noticeable trails in a Humvee," said Keane. "But, after I realized we had a GPS unit in the vehicle, I felt a lot better."

Just when the chief was getting used to the cool Korean climate, it was off to Kadena Air Base, Okinawa, home of the 390th Intelligence Squadron.

Here, Keane experienced another first when he donned headsets and attempted to copy code and translate foreign languages during a simulated mission. It didn't take long for the chief to understand why the training regimen for many of the airborne operators was so intense.

And, it only took a few moments to realize that without the countless "behind-the-scenes" support personnel, no mission would ever occur. To round out his Kadena leg of the trip, Keane spent time visiting with members of the 82nd Reconnaissance Squadron.

Last stop, Hickam AFB, where the chief spent time on the weekend visiting shift workers, getting lessons on treaty compliance, learning about communications monitoring, and seeing how all the units he'd visited fit into the overall mission of the 692nd Information Operations Group. For many of the group's senior NCOs, the highlight of the trip was when the chief shared his thoughts on leadership during the group's Senior NCO Investiture Ceremony.

With the "PACAF Tour 2002" under his belt, Keane headed back to ACC headquarters with a better understanding of the roles and missions of some of ACC's PACAF-based units.

When his schedule permits, he plans a return trip to the remaining units he wasn't able to visit.

Air Force remains committed to AEF rotation cycles

By TSgt. Tim Dougherty
Air Force Print News

The combination of America's war on terrorism and steady state commitments worldwide has put increased strain on the Air Force's aerospace expeditionary forces. However, except for a few stressed career fields, officials at the Pentagon say normal rotations should be back soon.

"Air Force Chief of Staff Gen. John P. Jumper is committed to the AEF construct — a three-month deployment with a 12-month period at home," said Maj. Gen. Jeffrey B. Kohler, director of operational plans, deputy chief of staff for air and space operations.

"Given the war on terrorism, we had to go through a momentary blip in our rotation schedule," he said. "However, it looks like we're going to be on time in bringing home about 90 percent of the people who are currently deployed. We will rotate the forces deployed for operations Enduring Freedom, Northern Watch and Southern Watch so that those who deployed first will be allowed to rotate home first to the maximum extent possible."

There are some exceptions, Kohler said. While Air Force leaders are working hard to come up with a solution, a very small number of career fields may not be able to rotate as scheduled, he said.

"We know that there are some stressed career fields, such as security forces, combat communications and firefighters, that might have to stay a little longer," Kohler said. "But that's not to say that absolutely everyone in those career fields will be staying longer."

The deployment picture will start to come into focus by the middle of February when the Air Force begins scheduling for the rotation in March, he said.

"It might work out that only one or two unit type codes out of an entire civil engineering squadron might be the stressed career field," Kohler said. "We just don't know yet because we haven't gotten down to that level of fidelity."

The tremendous performance of the AEF in Operation Enduring Freedom is what caused the stress on certain career fields in the first place, Kohler said.

"The Air Force is sort of a victim of its own success," Kohler said. "The reason we are stressed is simple — we do such a great job. We went out and set up these bases and started generating sorties as soon as we were asked. I think the results speak for themselves in the war on terrorism in Afghanistan. The (U.S.) Central Command commander in chief could not have done what he did without the superb work of all the airmen who went out and set it up."

To ease the problems the Air Force has in stressed career fields under current requirements, about 10 percent of the people will stay deployed a little longer — some up to 135 days; others, up to 179 days, Kohler said. To cover the overlap, the second part of the solution will be to reach into the next AEF and bring replacement unit type codes forward about 45 days. Any reduction in current requirements may get the AEF cycle on track a little bit quicker, he said.

Another way to relieve some of the burden on our deployed people is to find additional airmen who normally do not deploy and place them in an AEF library.

"This crisis has caused us to look a little bit deeper," Kohler said. "We'd like to be able to find people who we haven't originally had in an AEF library who can deploy but normally don't deploy. For example, Air Education and Training Command has instructors who have special skill sets, and the AETC leadership has said that there may be periods in the year when they can rotate. This is just one example and we're looking at all options."

Other fixes for stressed career fields are going to take some time and may only be resolved with increased manpower. Although the Air Force has asked for an end-strength increase of about 22,000 with 7,000 requested for this year, because of training requirements, this is more of a long-term solution, Kohler said.

"This is an extraordinary time for the Air Force and our country," Jumper recently told commanders. "The nation is grateful for the sacrifices our airmen continue to make in meeting our commitments to fight the war on terrorism and defend the American homeland. The secretary and I are proud of the job you are doing and we are personally committed to maintaining the AEF rotation schedule to the greatest possible extent."

Lawful terror: The Cheka

By Dr. Dennis F. Casey
HQ AIA/HO
Lackland AFB, Texas

Dec. 20, 1917, a new organization surfaced in revolutionary Russia. In time it would become the largest political police force in the world and at the same time the largest foreign intelligence service in the world.

Vladimir Ilyich Lenin would not have initially conceived of such an organization ever being developed or for that matter even being necessary before the Bolshevik Revolution of October 1917.

When Lenin passed through Finland station in April 1917, just two months after the February Revolution that had overthrown the Tsar, he was convinced their own revolution would spark an international revolutionary movement that eventually would cause the collapse of world capitalism.

Both Lenin and Leon Trotsky felt that in the new post revolutionary order there would be no need for diplomats and certainly not spies. When Trotsky became the People's Commissar for Foreign Affairs he proudly affirmed that ""I will issue a few proclamations to the peoples of the world and then shut up shop." He then went on to announce the abolition in Russia of secret diplomacy.

Lenin confirmed Trotsky's view of essentially a utopian Russia. In his State and Revolution written in the summer of 1917, he persuaded his readers that Russia's new order would not require the services of a police force and most certainly not those of a secret police organization. Lenin went on to explain that the people would dispense with class justice in the street.

Despite such claims that assumed a solid political position, the Bolsheviks had to contend with the fact that they had gained support but were far from having complete political control. In the post revolutionary elections to the Constituent Assembly, the Socialist Revolutionaries gained an absolute majority while the Bolsheviks garnered less than a quarter of the vote.

Convinced that all opposition was counterrevolutionary, the Bolshevik leadership created the Commission for Combating Counterrevolution and Sabotage Dec. 4, 1918.

Felix Dzerzhinsky received the nod to head the new organization. When it looked like a strike threatened to undermine the entire Bolshevik structure, Dzerzhinsky was ordered to create the All Russian Extraordinary Commission for Combating Counterrevolution and Sabotage or Cheka.

Years after his death, Felix Dzerzhinsky would be placed in the KGB pantheon of heroic figures of the Russian revolution. His status in 1918 was far simpler. Like many of the early leaders of the Cheka, he was not a Russian. He saw the first light of day in 1877 when he joined a family of wealthy Polish landowners and intelligentsia.

As a child he believed God had called him to become a Catholic priest. Instead he became a young convert to Marxism and in 1895 joined the Lithuanian Social Democratic Party. He soon abandoned his formal education and decided to pursue a much more practical life's course by joining the masses. Five years later he was known as an accomplished agitator and one of the founders of the Social Democratic Party of the Kingdom of Poland and Lithuania. His outspoken support of revolutionary causes landed him in prison.

The nearly twenty years of incarceration would have stilled the revolutionary ardor of most but not Dzerzhinsky. Once released from prison after the fall of the Tsar in February 1917, he joined the Bolsheviks and took part in the October Revolution.

His endurance and his selfless life style brought him the nickname of Iron Felix. Like Lenin, the Cheka leader was ready to sacrifice himself for the revolution. No one espoused better the Bolshevik doctrine.

Dzerzhinsky was probably best described by his contemporaries as a steadfast workaholic. During his first year as head of the Cheka, he ate, worked, and slept in his office in the Lubyanka, once the offices of Lloyds of London.

His endurance and his selfless life style brought him the nickname of Iron Felix. Like Lenin, the Cheka leader was ready to sacrifice himself for the revolution. No one espoused better the Bolshevik doctrine.

During his first year at the helm of the Cheka, he supported the uses of seizure of property, resettlement, deprivation of ration cards, publication of lists of enemies of the state and an impressive assortment of other measures. All focused on gaining political power for the Bolsheviks.

The main weapon, however, was terror. Once Lenin became fully aware of the opposition to the Bolsheviks, his thinking evolved into a position that supported the use of terror to achieve party objectives.

Dzerzhinsky and many of his associates believed that the use of terror was not directed against individuals but against bourgeoisie as a class. It was class warfare. For the

recipients of Cheka attention, their treatment became very personal. When the extent of their brutality became known publicly, Dzerzhinsky explained it as being nothing more than bloodthirsty impulses. These impulses in Moscow brought unfavorable reactions.

When the Cheka opened for business in Moscow, their list of candidates to receive brutal treatment was extensive. Heading the list was the celebrated circus clown Bim Bom. His repertoire included jokes about the Bolsheviks in particular and Communists in general.

When Cheka agents attempted to arrest the irreverent clown during one of his performances, the audience thought the antics were part of the act. Bim Bom fled from the ring with the agents firing at him. His escape was made possible when the audience in panic bolted for the exits. As one amused bystander so aptly put it, the clowns were chasing the clown.

The Cheka did not devote all of its energies to the pursuit of enemies of the state.

In 1918 it kicked off penetration operations. Its efforts were rewarded relatively early with the exposure in the summer of 1918 of what became known as the Lockhart Plot.

Robert Bruce Lockhart was the acting British consul-general in pre-Revolutionary Moscow. He had been an able official in the consular service but twice his career had been interrupted by torrid love affairs.

At the beginning of 1918 Lockhart was sent back to Russia to make contact with the new Bolshevik regime. His mission was to convince Lenin and the other leadership to continue the war with Germany. His mission ended in failure. Even after the peace of Brest-Litovsk, Lockhart maintained it was still possible to mount an offensive against Germany. Leon Trotsky, then the commissar of war, desperately wanted to keep the lines open with Great Britain so he encouraged Lockhart in his thinking. No such opportunity, however, ever existed.

When Lockhart finally realized that there existed no hope whatever of reviving the war on the eastern front, he became a rabid anti-Bolshevik.

By May 1918 Lockhart had established contact with agents of the anti-Bolshevik underground. He forwarded a plan to London to murder all of the Bolshevik leadership should the Allies elect to intervene on May 23, 1918.

Agents from the British Secret Intelligence Service, then known as MI1c, began to enter Moscow but met with the acid tongue of Lockhart who saw them as untrained and incompetent. While Lockhart might have been correct in his assessment, Cheka leaders concluded that the agents represented only a part of a massive effort by Western intelligence services. They would take seriously Lockhart's machinations.

While it was true that Lockhart did not think much of British intelligence agents serving in Moscow, he did allow for one notable exception.

Sidney Reilly captivated him. Born Sigmund Rosenblum in 1874, the only son of a wealthy Polish Jew, Reilly's career had been nothing short of miraculous in Lockhart's view. Breaking off all contact with his family, Reilly emigrated to London and by the 1890s had acquired the reputation of being self-confident, an international adventurer, and in the words of some who knew him better than others, an expert in sexual seduction.

Despite his reputation, he possessed a flair for intelligence and an indifference to danger. This combination of talent would win him the admiration of Sir Mansfield Cumming, the first head of the British Secret Intelligence Service and none other than Winston Churchill.

By the spring of 1918 Reilly had set himself up in Moscow as a businessman and a renowned bigamist. Because of his personal flamboyance, Reilly was only employed as a casual or part-time agent.

By July 1918 Lockhart had become deeply involved in supporting plots to overthrow the Communist regime. In concert with the French consul-general in Moscow, Fernand Grenard, the two handed out over 10 million rubles to the National Center in Moscow which was closely linked to the White Army of Tsarist General Alekseev.

Lockhart, even with his unusual combination of talents and avocations, was no match for Dzerzhinsky.

Within months a Cheka agent named Col. Eduard Berzin had penetrated Lockhart's inner circle which now included Reilly. Colonel Berzin who commanded one of the regiments of the Praetorian Guard of the Soviet Government convinced the conspirators that his troops were ready to participate in a coup d' etat.

Through the summer Dzerzhinsky played a game of cat and mouse with Lockhart and his friends. Just when he was about to have the conspirators arrested Aug. 30, 1918, Lenin was shot and seriously wounded by a deranged revolutionary named Fanya Kaplan. On the same day a military cadet assassinated the head of the Petrograd Cheka. The two unconnected events produced a reign of terror by the Cheka.

Beginning Aug. 31, Cheka agents systematically began liquidating what was called the Lockhart conspiracy. Reilly escaped but the American agent, Kalamatino, then posing as a Russian engineer under the name of Serpovsky, was apprehended.

A hollow cane found in his apartment contained a list of all those who had received payments for providing him with information. The list told it all. The only one of the conspirators who could claim diplomatic immunity was Lockhhart.

Fanya Kaplan was shot in a Kremlin courtyard just days after Lockhart's release, not knowing if her

effort to assassinate Lenin had been successful or not.

Cheka agents raided several sites expecting to pick up conspirators unaware that they were being closely watched Sept. 1.

When they found explosives for use in sabotage operations in one suspected agent's apartment, the Cheka leadership became convinced they had uncovered an extensive plot financed by the French and the British to discredit the Russian state if not bring about its collapse.

The Cheka disclosed their findings and went public, naming Lockhart and Grenard as the heads of the conspiracy Sept. 2.

In the days that followed, the Cheka arrested several of Reilly's mistresses but could not find the illusive Reilly. He had obtained a forged passport and had left Russia aboard a Dutch freighter bound for England.

Lockhart, after a time in prison was released and also returned to England.

The Cheka proclaimed its breaking up of the Lockhart conspiracy as a major victory. In reality it was not.

They had been unable to uncover the inner workings of the covert organization and pinpoint many of those involved. The experience, however, had been seminal in Dzerzhinsky's development of the idea that the Cheka should exercise total supervision over Soviet society. This totalitarian vision would become central to the development of the Stalinist police state that would emerge in the 1930s.

From 1917 to 1921 the Cheka, in attempting to secure power for the Bolsheviks, probably executed more than 250,000 people. Most were charged with treason but many not at all.

Under Dzerzhinsky's leadership, the terror they wielded was complete. Those meeting their fate shared the common characteristic of being opposed to Bolshevism.

With the Bolshevik victory secure in 1921, many in the party believed the Cheka had outlived its usefulness. Their methods had been at times excessive.

It was accordingly reduced in size and its responsibilities curtailed in 1921. It remained active but on a reduced scale until Feb. 8, 1922 when it was replaced by the State Political Directorate or GPU.

Felix Dzerzhinsky would remain in control of the GPU until his death July 20, 1926 of a fatal heart attack.

Reilly would be lured back into Russia in 1925 where he was arrested and executed after he had provided his captors a list of his contacts within Russia.

In keeping with his nearly miraculous abilities to manipulate, Lockhart would fade into the English landscape. In contrast, the Cheka would disappear only to be reborn and heralded as the foundation for the modern KGB.

salutes

QUARTERLY AWARDS

694th SPTS Airman
SrA. Roger Larew
694th SPTS

694th SPTS NCO
TSgt. Mitchell Ross
694th IG

694th SPTS SNCO
MSgt. Ronald Hill
694th SPTS

694th SPTS CGO
1st Lt. Eve Anderson
694th IG

694th SPTS Civilian
Patrice Andrews
694th IG

NAIC Airman
SrA. Heather Goldie

NAIC NCO
TSgt. Lee Young

NAIC SNCO
MSgt. Dennis Reed

NAIC CGO
Capt. Travis Blake

NAIC Airman
A1C Linda Felts

NAIC NCO
SSgt. David Southfall

NAIC SNCO
MSgt. Gary Koble

NAIC CGO
1st Lt. Jeanette Skow

690th CSS Airman
A1C Abdul Khandker

690th CSS NCO
SSgt. Scott Mann

690th CSS *SNCO*
MSgt. Nerlen Glaspie

690th CSS CGO
Capt. Steven Phelps

690th CSS Jr. Civilian
Mr. Randy Cox

690th CSS Senior Civilian
Mr. James McCollom

690th IOG NCO
SSgt. Scott Mann

690th IOG CGO
Capt. Steven Phelps

26th IOG Airman
A1C Carmeisha Layton
488th IS

26th IOG NCO
SSgt. Wendy Crawford
451st IOS

26th IOG SNCO
MSgt. James Bovenkerk
488th IS

26th IOG CGO
Capt. Vaughn R. Heyer
451st IOS

26th IOG Civilian
Mr. John Cherry
426th IOS

26th IOG Jr. Tech
SrA. Lori Nichter
426th IOS

26th IOG Sr. Tech
TSgt. John Benner
488th IS

485th IS Jr. Technician
A1C Nova Rogers

485th IS Airman
A1C Kisia Lamkin

485th IS Sr. Technician
SSgt. Floyd Easley

485th IS NCO
SSgt. Chris Penberthy

26th IOG staff NCO
TSgt. Edward Sutton

26th IOG staff SNCO
MSgt. Michael Ronayne

26th IOG staff Sr. Technician
SSgt. Peter Quarker

ANNUAL AWARDS

694th SPTS Airman
SrA. Diane Creek
694 SPTS

694th SPTS NCO
SSgt. Shelley Price
694 SPTS

694th SPTS SNCO
MSgt. Brian Howard
694th SPTS

694th SPTS CGO
2nd Lt. Kenneth Toso
694th IG

694th SPTS Civilian
Robert Effler
694th IG

543rd IG Outstanding Supply Personnel
TSgt. Maceo Lynch
MSgt. Thomas Zabel

543rd IG Communications Information Personnel
A1C Jayson Harper
TSgt. Donald Johnson
MSgt. Steven Potts

543rd IG Intelligence
SrA. Richard Badgley
SSgt. Jason Gifford
MSgt. Victor Cortes
Capt. Patrick Weldon
Maj. Scott Muessig

93rd IS Airman
SSgt. Candace Hatton

93rd IS NCO
SSgt. Tanya Keck

93rd IS SNCO
SMSgt. Reginald Smith

93rd IS CGO
1st Lt. Eric Allen

93rd IS Civilian
Ricardo Martinez

690th CSS Airman
A1C Abdul Khandker

690th CSS NCO
SSgt. Ben Wallis

690th CSS SNCO
MSgt. Nerlen Glaspie

690th CSS CGO
Capt. John Rosbrugh

690th CSS Junior Civilian
Mr. Randy Cox

690th CSS Senior Civilian
Mr. Calvin Bryant

690th CSS Supervisory Civilian
Mr. Ladd Smith

690th IOG Airman
A1C Abdul Khandker

690th IOG NCO
SSgt. Ben Wallis

690th IOG Junior Civilian
Mr. Randy Cox

690th CSS Comm and Info Airman
A1C Abdul Khandker

690th CSS_Comm and Info NCO
SSgt. Scott Mann

690th CSS Comm and Info SNCO
SMSgt. Jesse Davis

690th CSS_Comm and Info CGO
Capt. Doug Short

690th CSSComm and Info Jr. Civilian
Mr. Randy Cox

690th IOG Comm and Info CGO
Capt. Doug Short

690th IOG Comm and Info Jr. Civilian
Mr. Randy Cox

690th CSS Jr. Technician
A1C Abdul Khandker

690th CSS Sr. Technician
TSgt. David Gorham

Det 2, 26th IOG Airman
A1C Ryan Rode

Det 2, 26th IOG SNCO
MSgt. Scott Van Voorst

Det 2, 26th IOG Jr. Technician
A1C Ryan Rode

Det 2, 26th IOG Sr. Tech.
TSgt. Tracy Currier

26th IOG staff Airman
A1C Kip Sawaya

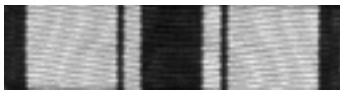
26th IOG staff NCO
TSgt. Edward Sutton

26th IOG staff SNCO
MSgt. Anthony Buono

26th IOG staff CGO
Capt. Joye Davis-Kirchner

26th IOG staff Jr. Tech
A1C Kip Sawaya

26th IOG staff Sr. Tech
TSgt. Gregory Floyd

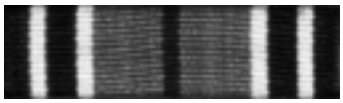


Air Force
Commendation Medal

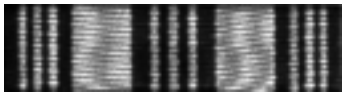
93rd IS
TSgt. Horneker, Theordore
SSgt. Moore, Craig

31st IS
SSgt. Dunfee, Hope
SSgt. Gifford, Jason

381st IS
SSgt. Atkinson, Phillip
SSgt. Clark, Joseph



Joint Service
Achievement Medal
381st IS
SSgt. Roberts, Troy



Air Force
Achievement Medal
381st IS
SrA. Golden, Debra
SrA. Mouton, Leo
SrA. Messinger, Michael